We claim:

1. In a processing system including a server capable of communicating with a client via a communications channel, a method of authenticating a data object, the method comprising the steps of, in the server,

(1) receiving the data object transmitted from the client to the server via the communications channel;

(2) generating a signature by processing the data object;

(3) associating the signature with the data object to create a signed object; and

(4) authenticating the signed object, subsequently upon request, by:

(a) deriving from the signed object information representative of the data object and the signature,

(b) generating a comparison value using the information representative of the data object,

(c) determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

2. The method of claim 1 wherein the data object comprises a document.

3. The method of claim 1 including the further step of, in the server, authenticating the client.

4. The method of claim 3 wherein the client is authenticated by the server using information representative of the client.

5. The method of claim 4 wherein the information representative of the client comprises a password provided by the client.

6. The method of claim 3 wherein the client is authenticated by the server using an encrypted data channel.

7. The method of claim 6 wherein the encrypted data channel utilizes a SSL protocol.

8. The method of claim 3 wherein the client is authenticated by the server using a public key-based processing step.

9. The method of claim 8 wherein the public key-based processing step includes the presentment of a client certificate.

10. The method of claim 9 wherein the client and server mutually authenticate using a zero-knowledge proof step.

11. The method of claim 3 including the further step of, in the server, creating and managing private keys to use in the step of generating the signature.

12. The method of claim 11 wherein the server assigns a private key to the client.

13. The method of claim 12 wherein the private key assigned to the client is determined based upon the information representative of the client.

14. The method of claim 13 wherein the step of generating the signature includes the steps of:

assigning a private key to the client;

performing a predefined hash function on the data object to produce a hash total; and

encyphering the hash total using the private key.

15. The method of claim 1 wherein the signed object comprises the signature and an address of the data object.

16. The system of claim 1 wherein the signed object comprises the signature and the data object.

17. In a processing system comprising a server capable of communicating with a client via a communications channel, a method of generating a digital signature, the method comprising the steps of, in the server:

receiving a data object transmitted from the client to the server via the communications channel;

assigning to the data object a descriptor containing a property field, the property field containing a signature field;

assigning a private key, stored at the server, to the client;

processing the data object using a pre-determined hash function and the private key to generate a signature; and

attaching the signature to the signature field associated with the data object to create a signed object.

18. The method of claim 17 including the step of, in the server, authenticating the signed object by verifying the signature attached to the signature field of the signed object.

19. The method of claim 18 wherein the verifying step further comprises the steps of:

(a) obtaining the data object from the signed object;

(b) obtaining the signature from the signed object;

(c) obtaining the private key stored at the server used to generate the signature;

(d) processing the data object using a pre-determined hash function and the private key to generate a comparison value; and

(e) determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

20. The method of claim 19 wherein the property field further comprises a timestamp.

21. The method of claim 20 wherein the property field further comprises an identifier used to look up a key stored at the server.

22. The method of claim 19 wherein the property field further comprises key information used to generate the comparison value.

23. The method of claim 17 wherein the descriptor further comprises a plurality of property fields.

24. The method of claim 23 wherein at least one of the property fields further comprises data that is private to the server.

25. The method of claim 23 wherein at least one of the property fields further comprises additional data that is signed by a key private to the server.

26. The method of claim 25 wherein the additional data is derived by processing the data object using a pre-determined function.

27. The method of claim 26 wherein the pre-determined function is a hash function.

28. The method of claim 26 wherein the pre-determined function is a transform function.

29. The method of claim 25 wherein the additional data is obtained from a device.

30. The method of claim 29 wherein the device receives the data object prior to subsequent processing by the server.

31. The method of claim 29 wherein the device does not receive the data object.

32. The method of claim 29 wherein the device further comprises a device for generating a timestamp.

33. The method of claim 29 wherein the additional data, after being obtained from the device, is used by the server to generate the signature.

34. A method of transmitting transaction objects between a client and a server capable of communicating with the client via a communications channel, the method comprising the steps of:

receiving at the client, from the server, an HTML object having a header record and an HTML form tag distinct from the header record, the HTML form tag having an outformat field representative of an outgoing transmission cryptographic protocol,

receiving, at the client, input form data corresponding to the HTML form tag,

generating secure form data by applying the specified outgoing transmission security cryptographic protocol of the HTML form tag to the input form data, and

transmitting to the server a return message including the secure form data.

35. A computer implemented method of providing a digital signature system on a server for use by a remote client, the method comprising:

generating on the server a private key for a user on the client;

storing on the server the private key for the user;

generating a digital signature using the stored private key for a data object provided by the user; and

sending the digital signature to the client.

36. The method of claim 35 wherein the digital signature is contained within a signed object.

37. The method of claim 36 wherein generating the digital signature step further comprises:

performing a pre-defined hash function on the data object to create a hash value; and

performing a pre-defined encryption function using the private key on the hash value.

38. The method of claim 37 wherein the signed object comprises the digital signature and an address of the data object.

39. The method of claim 37 wherein the signed object comprises the digital signature and the data object.

40. The method of claim 37 wherein the signed object comprises the digital signature contained within the data object.

41. The method of claim 36 wherein the signed object comprises a hash of the data object contained within the digital signature.

42. The method of claim 37, further including, on the server:

verifying the digital signature upon request by the client.

43. The method of claim 42 wherein verifying the digital signature further comprises:

receiving the signed object from the client;

obtaining the data object using information contained within the signed object;

obtaining the digital signature using information contained within the signed object;

obtaining the private key stored on the server using information contained within the signed object;

generating a comparison value using the data object;

verifying the digital signature if the comparison value and at least a portion of the digital signature meet a pre-determined criteria.

44. The method of claim 43 wherein the signed object comprises the digital signature and an address of the data object.

45. The method of claim 43 wherein the signed object comprises the digital signature and the data object.

46. The method of claim 43 wherein the signed object comprises the digital signature contained within the data object.

47. The method of claim 43 wherein the signed object comprises a hash of the data object contained within the digital signature.

48. The method of claim 35 further comprising, authenticating a user, by the server, before providing access to the system.

49. The method of claim 48 wherein authenticating a user further comprises receiving a user ID and a password from the client.

50. The method of claim 49 further comprising assigning, by the server, a private key to the client based upon the user ID.

51. The method of claim 35 further comprising assigning, by the server, a private key to the client based upon a system policy and data obtained from the client.

52. The method of claim 50 wherein the digital signature further comprises:
a encrypted field; and
a timestamp,
wherein the server generates the encrypted field by hashing the data object according to a predefined hash function to create a hash, and encrypting the hash using the private key assigned to the user.

53. The method of claim 52 wherein the digital signature further comprises a server key.

54. The method of claim 43 further including generating a verification response at the server and transmitting the verification response to the client.

55. The method of claim 54 further including generating a verification signature for the verification response at the server and transmitting the verification signature to the client.

56. A digital signature system including:

a server capable of communicating with a client via a communications channel, and means for authenticating a data object, further comprising:

(1) means for receiving the data object transmitted from the client to the server via the communications channel;

(2) means for generating a signature by processing the data object;

(3) means for associating the signature with the data object to create a signed object; and

(4) means for authenticating the signed object, subsequently upon request, by: (a) deriving from the signed object information representative of the data object and the signature,

(b) generating a comparison value using the information representative of the data object,

(c) determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

57. The system of claim 56 wherein the data object comprises a document.

58. The system of claim 56 further comprising means for obtaining information representative of the client to authenticate the client.

59. The system of claim 58 further comprising means for creating and managing private keys used to generate the signature.

60. The system of claim 59 further comprising means for assigning a private key to the client.

61. The system of claim 60 wherein the private key is assigned to the client using the information representative of the client.

62. The system of claim 56 wherein the means for generating a signature further comprise:
assigning a private key to the client;
performing a predefined hash function on the data object to produce a hash total; and
encyphering the hash total using the private key.

63. The system of claim 56 wherein the signed object comprises the signature and an address of the data object.

64. The system of claim 56 wherein the signed object comprises the signature and the data object.

65. A processing system comprising:

a server capable of communicating with a client via a communications channel, processing means in the server for generating a digital signature, further comprising:

means for receiving a data object transmitted from the client to the server via the communications channel;

means for assigning to the data object a descriptor containing a property field, the property field containing a signature field;

means for assigning a private key, stored at the server, to the client;

means for processing the data object using a pre-determined hash function and the private key to generate a signature; and

means for attaching the signature to the signature field associated with the data object to create a signed object.

66. The processing system of claim 65 further comprising means for authenticating the signed object.

67. The processing system of claim 66 wherein the means for authenticating the signed object is further comprised of means for verifying the signature attached to the signature field of the signed object.

68. The processing system of claim 67 wherein the means for verifying further comprises:

(a) means for obtaining the data object from the signed object;

(b) means for obtaining the signature from the signed object;

(c) means for obtaining the private key stored at the server used to generate the signature;

(d) means for processing the data object using a pre-determined hash function and the private key to generate a comparison value; and

(e) means for determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

69. The processing system of claim 67 wherein the property field further comprises a timestamp.

70. The processing system of claim 67 wherein the property field further comprises an identifier used to look up a key stored at the server.

71. The processing system of claim 67 wherein the property field further comprises key information used to generate the comparison value.

72. The processing system of claim 67 wherein the descriptor further comprises a plurality of property fields.

73. The processing system of claim 72 wherein at least one of the property fields further comprises data that is private to the server.

74. The processing system of claim 72 wherein at least one of the property fields further comprises additional data that is signed by a key private to the server.

75. The processing system of claim 74 wherein the additional data is derived by processing the data object using a pre-determined function.

76. The processing system of claim 75 wherein the pre-determined function is a hash function.

77. The processing system of claim 75 wherein the pre-determined function is a transform function.

78. The processing system of claim 74 further comprising a device for providing the additional data.

79. The processing system of claim 74 wherein the device receives the data object prior to subsequent processing by the server.

80. The processing system of claim 74 wherein the device does not receive the data object.

81. The processing system of claim 74 wherein the device further comprises a device for generating a timestamp.

82. The processing system of claim 74 wherein the server generates the signature after obtaining the the timestamp from the device.

83. A digital signature system for use by a remote client, the system comprising:
a server computer;
processing means on the server for generating a private key for a user on the client;
storing means on the server for storing the private key for the user;
processing means for generating a digital signature using the stored private key for a data object provided by the user; and
transmitting means for sending the digital signature from the server to the client.

84. The digital signature system of claim 83 wherein the digital signature is contained within a signed object.

85. The digital signature system of claim 84 wherein the processing means for generating the digital signature further comprise:
means for performing a pre-defined hash function on the data object to create a hash value; and

means for performing a pre-defined encryption function using the private key on the hash value.

86. The digital signature system of claim 85 wherein the signed object comprises the digital signature and an address of the data object.

87. The digital signature system of claim 85 wherein the signed object comprises the digital signature and the data object.

88. The digital signature system of claim 85 wherein the signed object comprises the digital signature contained within the data object.

89. The digital signature system of claim 85 wherein the signed object comprises a hash of the data object contained within the digital signature.

90. The digital signature system of claim 85, further comprising:

verifying the digital signature upon request by the client.

91. The digital signature system of claim 90 wherein the means for verifying the digital signature further comprises:

means for receiving the signed object from the client;

means for obtaining the data object using information contained within the signed object;

means for obtaining the digital signature using information contained within the signed object;

means for obtaining the private key stored on the server using information contained within the signed object;

means for generating a comparison value using the data object;

means for verifying the digital signature if the comparison value and at least a portion of the digital signature meet a pre-determined criteria.

92. The digital signature system of claim 91 wherein the signed object comprises the digital signature and an address of the data object.

93. The digital signature system of claim 91 wherein the signed object comprises the digital signature and the data object.

94. The digital signature system of claim 91 wherein the signed object comprises the digital signature contained within the data object.

95. The digital signature system of claim 91 wherein the signed object comprises a hash of the data object contained within the digital signature.

96. The digital signature system of claim 91 further comprising means for authenticating a user before providing access to the system.

97. The digital signature system of claim 96 wherein means for authenticating a user further comprises means for receiving a user ID and a password from the client.

98. The digital signature system of claim 97 wherein the server assigns a private key to the client based upon the user ID.

99. The digital signature system of claim 98 wherein the server assigns a private key to the client based upon a system policy and data obtained from the client.

100. The digital signature system of claim 91 wherein the digital signature further comprises:

a encrypted field; and

a timestamp,

wherein the server generates the encrypted field by hashing the data object according to a predefined hash function to create a hash, and encrypts the hash using the private key assigned to the user.

101. The digital signature system of claim 91 wherein the digital signature further comprises a server key.

102. The digital signature system of claim 100 further comprising:

means for generating a verification response at the server; and

means for transmitting the verification response to the client.

103. The digital signature system of claim 100 further comprising:

means for generating a verification signature for the verification response at the server; and

means for transmitting the verification signature to the client.